МКБ

Как обеспечить безопасность заказной разработки

POV Банка

Валерий Лобанов
к.т.н., PMP, ITBP @ МКВ

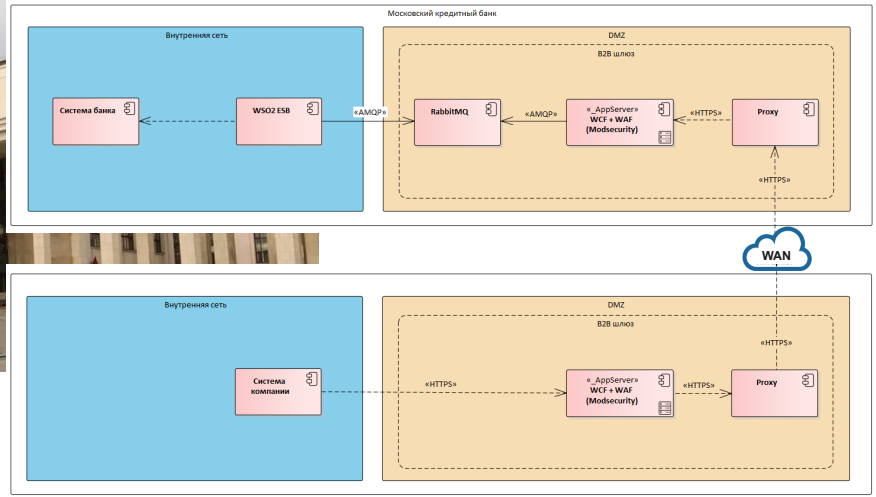
Заказная разработка в Банке

Тендер

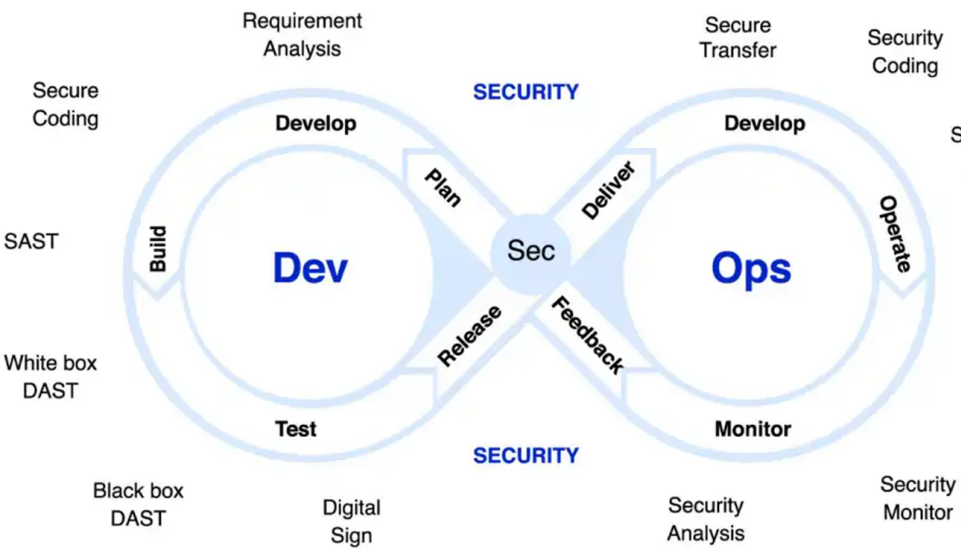
ВНД

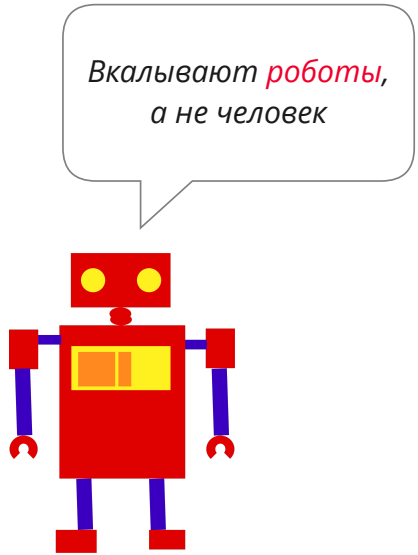
Тендер: общие и спец требования

Библиотека паттернов интеграции

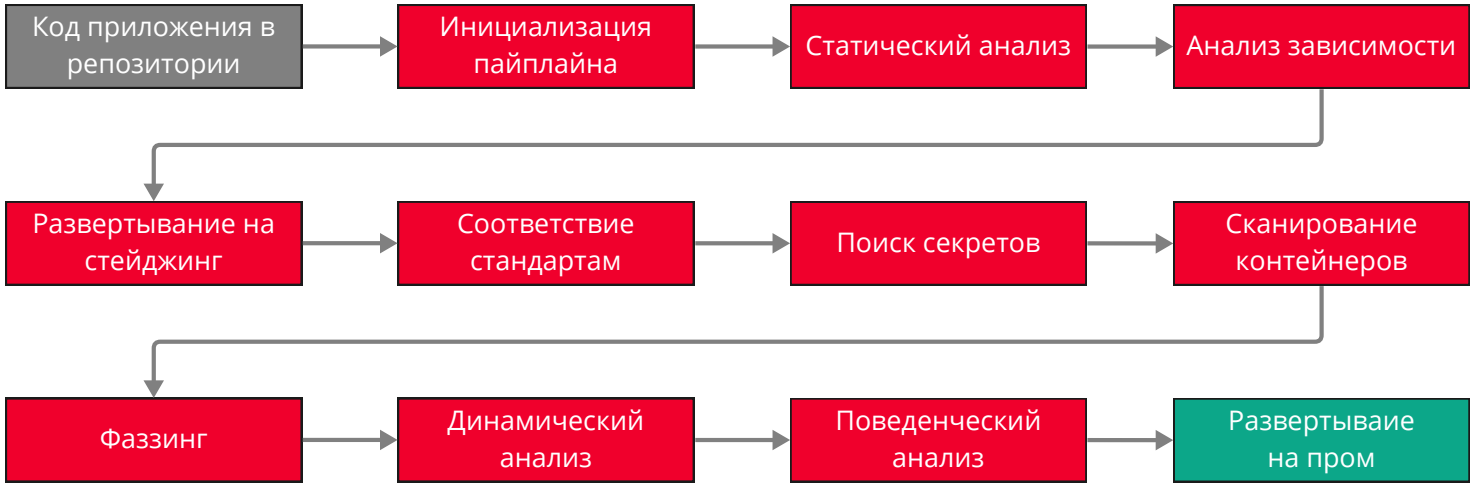


DevSecOps - как ДевОпс, только Сек





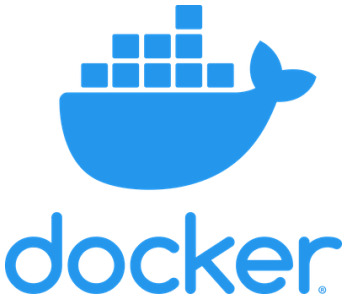
OWASP DevSecOps guideline



Бинарные артефакты

Ручной контроль	Автоматизация
Выпуск вендором новой библиотеки. Уведомление о выпуске.	Регулярная синхронизация с целевым ресурсом для размещения библиотек у вендора
Передача библиотеки на проверку	Получение библиотеки при появлении новой версии
Создание заявок /согласование заявок / назначение исполнителя	Запуск и выполнение процедур проверки библиотеки
Проверка/экспертиза/результат (принятие решения)	Проверка/экспертиза/результат (принятие решения)
Передача библиотеки эксплуатанту || передача найденных уязвимостей вендору	Размещение библиотеки на целевом внутрибанковском ресурсе с информированием заказчика || передача найденных уязвимостей вендору
У НАС - ПЕРЕПИСКИ / ВСТРЕЧИ / СОЗВОНЫ	У НАС – СВОБОДНОЕ ВРЕМЯ ДЛЯ СЛОЖНЫХ ЗАДАЧ
ДНИ	ЧАСЫ / МИНУТЫ

Контейнеры

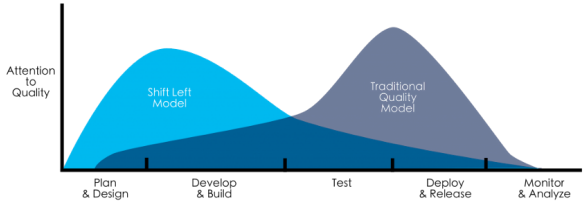


Ручной процесс	Автоматизированный процесс
Несколько десятков образов в репозиториях у вендора	Настройка синхронизации с репозиторием вендора
Выделение/настройка технических ресурсов для проведения проверок	Регулярное получение статусов по размещенным образам (новые/уже проверенные)
Создание заявок /согласование заявок / назначение исполнителя	Запуск и выполнение процедур проверки образов
Проверка/экспертиза/результат (принятие решения)	Проверка/экспертиза/результат (принятие решения)
Передача образов эксплуатанту || передача найденных уязвимостей вендору	Размещение образов в целевом внутрибанковском репозитории с информированием заказчика | инфоормирование вендора о найденных уязвимостях
При любых изменениях в составе образов – повторить все перечисленные действия N раз	При любых изменениях в составе образов – получить новые результаты на экспертизу
ДНИ	ЧАСЫ / МИНУТЫ

Ни шагу без искусственного интеллекта

И все же люди

Shift Left и обучение
Security Champions



МКБ

Я за безопасную разработку!

Валерий Лобанов, к.т.н., PMP
ITBP @ МКВ
+7 (916) 012 40 76